

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-166029

(43)Date of publication of application : 10.06.2004

(51)Int.Cl.

H04L 12/66
H04L 12/56

(21)Application number : 2002-330277

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 14.11.2002

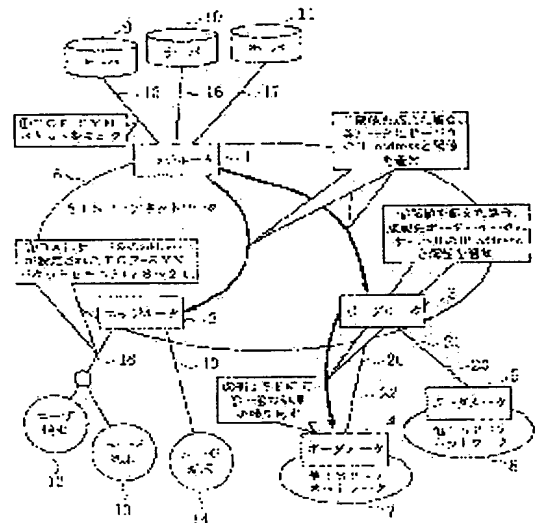
(72)Inventor : KANEKO HITOSHI
TOYOSHIMA AKIRA

(54) METHOD, SYSTEM AND PROGRAM FOR CONTROLLING DISTRIBUTED SERVICE REJECTION

(57)Abstract:

PROBLEM TO BE SOLVED: To minimize DDoS attack countermeasure processing in a network, to perform necessary processing, to provide a plan for obtaining an effect, to expand a processing range even to other ISPs and to apply accurate processing even to an attack packet that flows in from the other ISPs.

SOLUTION: Exit lines 15 to 17 on a server side of an edge router 1 in an ISP to which servers 9 to 11 to be a protection target, lines 18 and 19 on a user terminal side of each edge router 2 in a self-ISP 6 that houses user terminals 12 to 14, and lines 20 and 21 to other ISPs 7 and 8 of a border router 3 are selected. In processing at a normal time, a threshold for the maximum traffic of a TCP-SYN that can accept a server to be protected is set in advance to perform monitoring. When traffic exceeds the threshold, a part that exceeds the threshold is filtered, and the address of the server and the threshold are notified to all subscriber housing edges and all border routers in the same ISP.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision of
rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-166029

(P2004-166029A)

(43) 公開日 平成16年6月10日(2004.6.10)

(51) Int. Cl.⁷

H04L 12/66

H04L 12/56

F 1

H04L 12/66

B

H04L 12/56

100Z

テーマコード (参考)

5K030

審査請求 未請求 請求項の数 7 O L (全 12 頁)

(21) 出願番号

特願2002-330277 (P2002-330277)

(22) 出願日

平成14年11月14日 (2002.11.14)

特許法第30条第1項適用申請有り 2002年8月20日 社団法人電子情報通信学会発行の「電子情報通信学会2002年ソサイエティ大会プログラム」に発表

(71) 出願人

000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(74) 代理人

100077274

弁理士 磯村 雅俊

(74) 代理人

100102587

弁理士 渡邊 昌幸

(72) 発明者

金子 斉

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72) 発明者

豊島 鑑

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

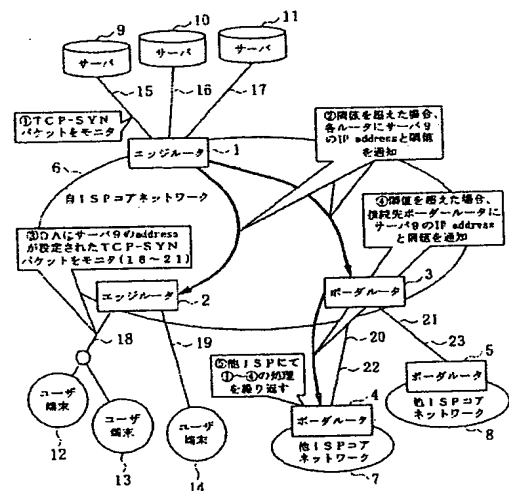
Fターム(参考) 5K030 GA15 HA08 HCO1 HD03 HD06
LB05 LC15 MA04 MB09

(54) 【発明の名称】 分散型サービス拒絶防御方法およびシステム、ならびにそのプログラム

(57) 【要約】

【課題】 ネットワーク内のDDoS攻撃対策処理を最小限に抑え、かつ必要な処理を行い、効果を得る方策を与え、かつ処理の範囲を他ISPにも拡張し、他ISPから流入する攻撃パケットについても的確な処理を行う。

【解決手段】 保護対象となるサーバ9～11が接続されるISP内のエッジルータ1のサーバ側の出口回線15～17、ユーザ端末12～14を収容する自ISP6内の各エッジルータ2のユーザ端末側の回線18、19、ボーダールータ3の他ISP7、8への回線20、21を選択する。平常時の処理としては、予め保護するサーバが受け付けられるTCP-SYNの最大トラヒックの閾値を設定しておき、モニタを行う。トラヒックが当該閾値を越えた場合、超えた分のフィルタリングを行い、同一ISP内の全加入者収容エッジおよび全ボーダールータへサーバのアドレスおよび当該閾値を通知する。



【特許請求の範囲】

【請求項 1】

IDC内のサーバマシンをTCP-SYN-Floodから保護するため、該IDCが接続されているISP網のエッジルータは、該IDC側の出口回線にて、該サーバマシンをdestination addressとするTCP-SYNパケットのトラヒックに対して閾値を設け、

該閾値を超えた場合に、超えた部分のトラヒックを廃棄し、

さらに、ユーザ端末を直接収容している各エッジルータおよびボーダールータに該閾値および該サーバマシンのaddressを通知し、

通知を受けた該エッジルータおよびボーダールータは、当該ISPとは反対側のインターフェースにて該閾値に基づくフィルタリングを行い、

さらに、該ボーダールータは、他ISPへのボーダールータに該閾値および該サーバマシンのaddressを通知し、

通知を受けた他ISPのボーダールータは、当該処理を繰り返し処理することを特徴とする分散型サービス拒絶防御方法。

【請求項 2】

前記IDCが接続されているISP網のエッジルータは、平常時の処理としては、予め保護するサーバが受け付けられるTCP-SYNの最大トラヒックの閾値を設定しておき、該閾値に基づいて単にモニタすることを中心とする請求項 1 記載の分散型サービス拒絶防御方法。

【請求項 3】

IDC内のサーバマシンに接続され、保護の対象であるサーバマシンをdestination addressとするTCP-SYNパケットのトラヒックに対して、予め定めた閾値を超えた部分のトラヒックを廃棄する自ISP網内のエッジルータと、

該エッジルータから前記閾値と前記サーバマシンのaddress情報を受信して、前記ISPの反対側のインターフェースで該閾値に基づくフィルタリングを行う、ユーザ端末を収容するエッジルータまたはボーダールータと、

該ボーダールータから前記閾値と前記サーバマシンのaddress情報を受信して、他ISPから自ISPの該ボーダールータ側のインターフェースで該閾値に基づくフィルタリングと前記各処理を行う他ISP網内のボーダールータとを有することを特徴とする分散型サービス拒絶防御システム。

【請求項 4】

自ISP網内のエッジルータに、IDC内の保護対象であるサーバマシンへの出口回線にて、該サーバマシンをdestination addressとするTCP-SYNパケットのトラヒックに対して閾値を設ける手

順、該閾値を超えた場合に超えた部分のトラヒックを廃棄する手順、ユーザ端末を直接収容する各エッジルータおよびボーダールータに該閾値と該サーバマシンのaddress情報を通知する手順を、実行させるためのプログラム。

【請求項 5】

ユーザ端末を直接収容している自ISP網内のエッジルータまたはボーダールータに、自ISP網内の他エッジルータから閾値とaddress情報を受信したことを確認する手順、当該ISPとは反対側のインターフェースにて該閾値に基づくフィルタリングを行う手順、直接収容している他ISPのボーダールータに対して該閾値とaddress情報を通知する手順を、実行させるためのプログラム。

【請求項 6】

他ISP網内のボーダールータに、自ISP網内のボーダールータから閾値とaddress情報を受信したことを確認する手順、他ISP網内のサーバマシンへの出口回線にて、該閾値に基づくフィルタリングを行う手段、他ISP網内のユーザ端末を直接収容するエッジルータおよびボーダールータに対して、該閾値とaddress情報を通知する手段を、実行させるためのプログラム。

【請求項 7】

請求項 4 から請求項 6 のいずれかに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ISP (Internet Service Provider) 網におけるDDoS (Defeating Denial of Service) 攻撃に対するインターネットセキュリティ向上技術に関し、特にDDoS攻撃に対する処理を最小限に止めることが可能な分散型サービス拒絶防御方法およびシステム、ならびにそのプログラムに関する。

【0002】

【従来の技術】

従来のDoS (Denial of Service) 攻撃に対する文献としては、2001年電子情報通信学会総合大会、B-7-14の岡田浩一、外1名『DoS攻撃のためのバックボーンネットワーク構築法』がある。DoS攻撃には、それに使用されるパケットを形式から判断できるもの(形式不正型)と、形式からは判断できないが、送信元のアドレスが特定範囲に限定されるもの(アドレス限定型)と、送信元アドレスが特定範囲に限定されないもの(アドレス不定型)とがある。形式不正型に対しては、バッチ当て、あるいはパターンマッチングによるフィルタリングで対処が可能である。

【0003】

また、アドレス限定型に対しては、IDS (Intrusion Detection System) による方法、つまり、特定範囲の送信元からのパケットの数が異常に多い場合、その範囲からのパケットの受信を制限または停止する対処法をとっている。アドレス不定型に対しては、上記文献により提案された方法、つまりイングレスフィルタリング装置を経由したパケットと、経由しないパケットを、パケットに安全性識別子を付加することで区別し、イングレスフィルタリング装置を経由したパケットを優先制御装置により優先してサーバに接続させる方法で対処する。

【0004】

しかし、比較的単純なDoS攻撃については、一般的に攻撃力が弱く、比較的前より対策手法がとられていたが、DDoS (Distributed DoS) に対しては、セキュリティ上脆弱な多数のPCを踏み台にして、一斉に攻撃を仕掛ける形態に進化しており、攻撃力は格段に増大している。

従来の方法では、TCP-SYN Floodの発見およびフィルタリング箇所として、保護対象のサーバが接続されるISP内のエッジルータか、あるいは、加入者を収容するISP内のエッジルータかのどちらか一方で、当該TCP-SYNパケットのフィルタリングが行われるため、発見の精度が低かったり、発見してもフィルタリングが一律的なものとなってしまう、いわゆる正当な使用者も含めてフィルタリングされてしまうという問題があった。

ここで、TCP-SYN-Floodとは、TCP (Transmission Control Protocol) パケットのフィールドのSYNの値にビットが立っているパケットを多量に送りつける攻撃のことである。

【0005】

また、ネットワークレベルで処理を行う場合、常時、ネットワーク全体の各エッジルータでトラヒック情報を収集し、各ルーター間でトラヒック情報などを通知し合うなどして全ルータにてトラヒック情報を共有し、DDoS攻撃の発見およびフィルタリングなどの対処を行う方式もある。しかし、収集するトラヒック情報の対象によっては、各エッジルータおよびネットワークの負荷が重いものになってしまう、あるいは、収集する情報の対象が狭い場合、発見の精度が落ちたり、また、フィルタリングの対象の絞り込みが不十分になったりする。また、ネットワークレベルで処理を行う場合でも、ISP内に閉じた処理であったため、トラヒック量として相当な量を占めるとされる他ISPからボーダールータを通して流入してくるTCP-SYN Floodに対しては、一律排除による手段を行うことになり、いわゆる正当なユーザのパケットも廃棄されてしまう。

【0006】

【非特許文献1】

2001年電子情報通信学会総合大会、B-7-14の岡田浩一、外1名『DoS攻撃のためのバックボーンネットワーク構築法』

【0007】

【発明が解決しようとする課題】

前述のように、発見の精度、つまり攻撃が行われた場合には、即発見し、攻撃が行われなかった場合には、発見と位置付けない処理、および、フィルタリングの精度、つまり必要のない場合にはフィルタリングは行わず、攻撃者のパケットと正常ユーザのパケットを区別する処理、の精度を上げるためには、ネットワーク内の処理について、負荷が重い処理となり、平常時のサービスに影響を与えてしまう、という問題点があった。

【0008】

本発明の目的は、このような問題点を解消し、ネットワーク内のDDoS攻撃対策処理を最小限に抑え、かつ必要な処理を行い、効果を得る方策を与え、かつ処理の範囲を他ISPにも拡張し、他ISPから流入する攻撃パケットについても的確な処理ができるような分散型サービス拒絶防御方法およびシステム、ならびにそのプログラムを提供することにある。

【0009】

【課題を解決するための手段】

本発明の分散型サービス拒絶防御方法は、まず、発見およびフィルタリングのポイントとして、保護対象となるサーバが接続されるISP内のエッジルータのサーバ側の出口回線、加入者を収容する自ISP内の各エッジルータの加入者側の回線、他ISPへの接続ポイントとなるボーダールータの他ISPへの回線を選択する。平常時の処理としては、予め保護するサーバが受け付けられるTCP-SYNの最大トラヒックの閾値を設定しておき、モニタを行う。平常時の処理は、以上のみである。

【0010】

トラヒックが当該閾値を越えた場合、超えた分のフィルタリングを行い、同一ISP内の全加入者収容エッジおよび全ボーダールータへサーバのアドレスおよび当該閾値を通知する。

通知を受けた加入者収容エッジルータおよびボーダールータは、当該閾（および、加入者収容エッジルータではフィルタリングを行うインターフェース毎の収容ユーザ数）を基に、当該フィルタリングの閾値を決め、超えているものについてはフィルタリングを行う。加入者収容エッジルータでは、フィルタリング可能な加入者側の各レイヤのインターフェースにて、インターフェースに収容されている加入者の数が最小になるようなインターフェースを選択する。

50 【0011】

各ボーダールータにおいて、トラヒックが閾値を超えてフィルタリングが行われた場合には、当該回線の接続先ISPのボーダールータにサーバのアドレスおよび閾値を通知する。通知を受けた他ISPでは、直接通知を受けたボーダールータを上記に記述したサーバ収容のエッジルータの位置付けとし、上記自ISPと同じ処理を行う。

【0012】

【発明の実施の形態】

以下、図7～図10により、DDoS攻撃対策を施さないネットワークでの説明を行い、その後、図1～図6によりDDoS攻撃対策を施した本発明の処理について説明する。

図7は、本発明の機能（DDoS攻撃対策機能）を施さないネットワークの図である。

自ISPコアネットワーク6において、縁の部分に位置するエッジルータ1、2およびボーダールータ3が配置されている。7、8は、他ISPのコアネットワークであって、4、5は縁の部分に位置するボーダールータである。

9、10、11は、IDC（Internet Data Center）内でeコマース、コンテンツ配信などを行うサーバマシンであり、12、13、14は自ISPに加入するユーザの端末である。15～17は、エッジルータ1におけるサーバ9～11側のインターフェース、18～19はエッジルータ2におけるユーザ端末12～14側のインターフェース、20～21は、ボーダールータ3における他ISPのボーダールータ側のインターフェース、22～23は、それぞれ他ISPのボーダールータ4、5における自ISPボーダールータ側のインターフェースである。

【0013】

図8は、IPヘッダーおよびTCPヘッダーのフィールドの図である。

TCP-SYNパケットは、図8に示すように、ProtocolはTCPを用い、flags-SYNはそれぞれ1ビットのパケットである。そして、IP header、TCP header、およびDataの順に送信される。TCP header内のflagsフィールド6ビット（ビット8～14）は、URG、ACK、PSH、RST、SYN、FINの6個の1ビットで構成される。

【0014】

以下、用語の説明を行う。まず、攻撃者はセキュリティ上脆弱なユーザ端末に侵入し、攻撃用のソフトウェアを埋め込むなどの攻撃の準備をする。図7では、進入されたユーザ端末を12および13、進入されなかったユーザ端末を14とする。また、ユーザ端末12、13のように、攻撃者に乗っ取られたユーザ端末を、以降は『ゾンビ』と呼ぶ。

【0015】

攻撃者は、乗っ取ったユーザ端末（図1の12、13）に対して、攻撃対象となるサーバ（図1の9）に対して一斉に多量のTCP-SYNパケットを送信するよう命令する。このとき、TCP-SYNパケットのsource address（送信元アドレス）にはランダム値が設定される。

一方、各攻撃端末よりの多量のTCP-SYNパケットを受け取ったサーバ9は、それぞれ1つずつのパケット毎にコネクションの処理に移る。この処理を、3way-handshakeと呼ぶ。

【0016】

図9は、正常な3way-handshakeのシーケンスチャートである。

3way-handshakeは、ユーザ端末12、13からサーバ9へ、TCP-SYNパケット（31）を送付する。TCP-SYNパケット（31）がサーバ9に送付されると、これを受信したサーバ9はパケットのsource

address先にTCP-ACK+SYNパケット（32）を返送する。

source addressに正しい値（12、13のIP address）が設定されていれば、当該パケットはユーザ端末12、13にたどり着き、当該パケットを受け取ったユーザ端末12、13は再度、TCP-ACKパケット（33）をサーバ9に返送し、これにてTCPコネクションが確立する（34）。

【0017】

しかし、通常ゾンビ12、13は、サーバ9にTCP-SYNパケットを送付する際に、source addressにランダム値を設定して送付するため、サーバ9は、そのランダム値のIP addressへTCP-ACK+SYNパケットを送付するため、当該パケットはゾンビ12、13にたどり着かない。

【0018】

図10は、ゾンビ12、13がサーバ9にTCP-SYNパケットを送付する場合のシーケンスチャートである。

ゾンビ12、13からTCP-SYNパケット（41）をサーバ9に送信する場合、ゾンビ12、13では、source addressにランダム値が設定されて送付されるので、サーバ9からTCP-ACK+SYNパケット（42）を返送する場合、ユーザ端末12、13とは別アドレスに送付されてしまう。従って、ユーザ端末12、13にはTCP-ACK+SYNパケット（42）は届かない。その結果、サーバ9にも、TCP-ACKパケット（43）は届かないことになる。従って、サーバ9は、タイムアウトするまでTCP-ACKパケット（43）の待ち状態となる。従って、多数のゾンビより当該多量のTCP-ACKパケットが送られる

ため、サーバ 9 は多数の待ち状態を維持することになり、リソース不足などにより機能停止してしまう。

【0019】

(実施例)

以下、本発明の実施例について説明する。

図 1 は、DDoS 攻撃対策を施した本発明の実施例を示すネットワーク図である。また、図 3 は、本発明のエッジルータにおけるフィルタリングのルール設定画面の例を示す図である。

ここでは、保護対象のサーバをサーバ 9 とする。まず、エッジルータ 1 におけるフィルタリングのルール設定を図 3 のように行う。エッジルータ 1 は、インターフェース 15 にてサーバ 9 の IP address を destination address に (53, 54)、PROTOCOL を TCP に (55) CONTROL FLAGS を SYN に (56)、一定の閾値を設け、閾値をオーバーする部分につきフィルタリングを行う。すなわち、DDoS 攻撃が行われても、トラヒック値が閾値の範囲内であれば、エッジルータ 1 は何の処理も行わない。

【0020】

閾値としては、予め当該サーバ 9 が正常運用可能なトラヒック値を設定しておく (57)。ここでは、予め 60 Kbps が設定されている。

また、トラヒックが閾値を超えた際に通知するルータの IP address も予め設定しておく (58)。通知先のルータについては、自ルータ以外の自 ISP コアネットワーク 6 内の全てのエッジルータおよびボーダールータの IP address を設定しておく。ここでは、111.11.22.3 と 22.22.33.4 が

設定されている。エッジルータ 1 は、トラヒック量が当該閾値を超えたとき、通知先に記してあるルータへ、当該閾値情報およびサーバ 9 の IP address 情報を添付して通知を行う。

【0021】

図 4、図 5 は、エッジルータ 2 およびボーダールータ 3 におけるフィルタリングルールの設定画面の例を示す図である。

図 4 において、通知を受けた各エッジルータおよびボーダールータ (図 1 の 2, 3) は、インターフェース 18 ~ 21 において送付された IP address を DESTINATION ADDRESS に (63)、PROTOCOL を TCP に (65)、CONTROL FLAGS を SYN に (66)、閾値を設け (67)、閾値をオーバーする部分についてフィルタリングを行う。このとき、エッジルータの対象となるインターフェースとしては、ユーザ端末に対してフィルタリング可能な、なるべく細かいインターフェースを選択する。図 4 では、VIRTUAL ROUTER の場合を例としてい

る (図 1 の 18)。図 4 の場合には、閾値を超えた場合にも、通知しない (68) ことに設定されている。なお、閾値としては、通知閾値 / 1000 が設定されている。

【0022】

図 5 においても、図 4 と同じように、インターフェース 18 ~ 21 において送付された IP address を DESTINATION ADDRESS に (73)、PROTOCOL を TCP に (75)、CONTROL FLAGS を SYN に (76)、閾値を設け (77)、閾値をオーバーする部分についてフィルタリングを行う。このとき、エッジルータの対象となるインターフェースとしては、ユーザ端末に対してフィルタリング可能な、なるべく細かいインターフェースを選択する。図 5 では、VIRTUAL ROUTER の場合を例としている (図 1 の 20)。閾値については、予め、通知された閾値と当該インターフェースに収容されるユーザ端末数を基にした計算式を記しておく (77)。ここでは、通知閾値 / 5 が設定されている。

【0023】

当該マシンがボーダールータの場合には、トラヒックが閾値を超えた場合の通知先 IP ADDRESS を記す (78)。通知先 IP ADDRESS には、当該インターフェースの接続先の他 ISP コアネットワークのボーダールータ (図 1 の 4, 5) のアドレスを記しておく。

ボーダールータは、ルールの記述に従って、トラヒックが閾値を超えた場合に接続先他 ISP のボーダールータに通知を行う。通知を受けたボーダールータ 4, 5 は、本処理の最初にエッジルータ 1 がインターフェース 15 を監視したのと同様に、それぞれインターフェース 22, 23 を監視し、他 ISP コアネットワーク内にて上記自 ISP と同様の処理を繰り返す。

【0024】

図 6 は、他 ISP のボーダールータにおけるフィルタリングのルール設定画面の例を示す図である。

図 6 の設定画面が、他と異なる点は、当該ボーダールータにて設定するルールにて、SOURCE ADDRESS は通知された IP address を用い、閾値は、通知された閾値を使用する点である。

すなわち、インターフェース 18 ~ 21 において送付された IP address を DESTINATION ADDRESS に (83)、PROTOCOL を TCP に (85)、CONTROL FLAGS を SYN に (86)、閾値は通知された閾値 (通知閾値) とし (87)、閾値をオーバーする部分についてフィルタリングを行う。図 6 でも、VIRTUAL ROUTER の場合を例としている (図 1 の 22)。図 6 の場合、通知先 IP ADDRESS には、当該インターフェースの接続先の他 ISP コアネットワークのボーダールータ (図

1の4, 5)のアドレスを記しておく(88)。

【0025】

図1に戻り、本発明の処理を説明する。

▲1▼エッジルータ1では、図3に示すルール設定画面により、インターフェース15でパケットのトラヒックが閾値を超えるか否かを監視(モニタ)する。

▲2▼閾値を超えた場合には、各ルータ(エッジルータ2、ボーダールータ3)にサーバ9のIP addressと閾値を通知する。

▲3▼エッジルータ2では、図4, 図5に示すルール設定画面により、DAにサーバ9のaddressが設定されたTCP-SYNパケットをインターフェース18~21でモニタ、すなわち、閾値を超えたか否かを監視する。

▲4▼閾値を超えた場合には、接続先ボーダールータにサーバ9のIP addressと閾値を通知する。

▲5▼他ISPのボーダールータ4, 5では、図6に示すルール設定画面により、上記▲1▼~▲4▼の処理を繰り返し行う。

【0026】

図2は、本発明の一実施例を示す分散型サービス拒絶防御方法の動作フローチャートである。

まず、エッジルータ1は、インターフェース15でDestination addressがサーバ9のIP address、protocolの値がTCP、Flagsの値がSYNであるパケットのトラヒックが閾値を超えるか否かを監視する(ステップ101)。

トラヒックが閾値を超えたならば(ステップ102)、超えた部分につき、パケットをフィルタリングする(ステップ103)。同一ISP内の各エッジルータに閾値、サーバ9のIPアドレスを通知する(ステップ104)。

【0027】

次に、エッジルータ2およびボーダールータ3のインターフェース18~21でDestination addressの値がサーバ9のIP address、protocolの値がTCP、flagsの値がSYNであるパケットのトラヒックが閾値(通知された閾値より計算)を超えるか否かを監視する(ステップ105)。

トラヒックが閾値を超えたならば(ステップ106)、超えた部分につき、パケットをフィルタリングする(ステップ107)。そして、自エッジルータの種類を判別し(ステップ108)、加入者収容エッジルータであれば、処理を終了し、ボーダールータであれば、他ISPボーダールータ(インターフェース20, 21の接続先)に閾値、サーバ9のIPアドレスを通知する(ステップ109)。

【0028】

次に、他ISPのボーダールータ4, 5は、自ISPコ

アネットワーク6にインターフェース15を、インターフェース22, 23に置き換えて、ステップ101~108の処理を実行する(ステップ110)。すなわち、ボーダールータ4, 5は、インターフェース22, 23でDestination addressがサーバ9のIP address、protocolの値がTCP、Flagsの値がSYNであるパケットのトラヒックが通知された閾値を超えるか否かを監視し(ステップ101)、トラヒックが閾値を超えたならば(ステップ102)、超えた部分につきパケットをフィルタリングし(ステップ103)、同一ISP内の各エッジルータおよびボーダールータに閾値、サーバ9のIPアドレスを通知する(ステップ104)。なお、図1には、記載が省略されているが、他ISPコアネットワーク7, 8にも、ユーザ端末が収容されるエッジルータが配置されている。また、ステップ110では、他ISPのコアネットワーク7, 8内に別のボーダールータがある限り、先へ先へと芋づる式に処理されることになる。この場合の全てのボーダールータは、図6に示すように、通知されたアドレス、閾値を利用する。

【0029】

他ISPのエッジルータおよびボーダールータのインターフェースでDestination addressの値がサーバ9のIP address、protocolの値がTCP、flagsの値がSYNであるパケットのトラヒックが通知された閾値を超えるか否かを監視し(ステップ105)、トラヒックが閾値を超えたならば(ステップ106)、超えた部分につき、パケットをフィルタリングし(ステップ107)、自エッジルータの種類を判別し(ステップ108)、加入者収容エッジルータのときは処理を終了し、ボーダールータのときには、他ISPボーダールータに閾値、サーバ9のIPアドレスを通知する(ステップ109)。

【0030】

なお、図2のフローにおいて、ステップ101~104は自ISPコアネットワークのエッジルータ1が実行すべきプログラムに変換することができ、ステップ105~109は自ISPコアネットワークのエッジルータ2およびボーダールータ3が実行すべきプログラムに変換することができ、ステップ110(ステップ101~109)は他ISPコアネットワークのボーダールータ4, 5が実行すべきプログラムに変換することができる。

そして、これらのプログラムをCD-RPMなどの記録媒体に格納しておけば、それを携帯してISPコアネットワークのエッジルータまたはボーダールータに装着することで、コンピュータにプログラムをインストールし、実行させることにより、本発明を容易に実現させることができる。

【0031】

【発明の効果】

以上説明したように、本発明によれば、DDoS攻撃に対する処理を最小限に止めることができる。すなわち、平常時には、エッジルータ1のみにて、サーバ9へのトラヒックを監視するのみである。DDoS攻撃が行われても、攻撃のトラヒックが限界値に達するまでは処理は行われない。攻撃のトラヒックが限界値を超えた場合でも、同一ISP内のエッジルータへの通知情報は極く少なく、ネットワーク負荷への影響も殆んどない。

【0032】

また、モニタ、フィルタリングがエッジルータ1とエッジルータ2、ボーダールータ3で2段階で実施されるため、エッジルータ2、ボーダールータ3のみで実施されるよりも発見の精度を高められ、処理の精度を高めることができる。

また、エッジルータ2、ボーダールータ3でのフィルタリング処理の閾値も高目に設定でき、正当ユーザへの影響を最小限に止めることができる。

フィルタリング処理をエッジルータ2、ボーダールータ3におけるフィルタリング処理を、自ISPコアネットワーク1と反対側の各インターフェース毎に行うため、攻撃者の絞り込みをすることができ、正当ユーザへの影響を最小限にすることができる。

【0033】

ボーダールータ間の通知を行うことにより、単に自ISPコアネットワークのボーダールータ3のみでフィルタリングを行う場合と比べて、接続先の他ISP7、8でも同様の処理が繰り返されることにより、攻撃元を更に絞り込むことができ、他ISPの正当ユーザも救済することができる。

【図面の簡単な説明】

【図1】本発明の一実施例を示す分散型サービス拒絶防御装置のネットワーク図である。

【図2】図1における分散型サービス拒絶防御方法の動作フローチャートである。

【図3】図1におけるエッジルータ1のルール設定画面

の例を示す図である。

【図4】図1におけるエッジルータ2のルール設定画面の例を示す図である。

【図5】図1におけるボーダールータ3のルール設定画面の例を示す図である。

【図6】図1におけるボーダールータ4でのルール設定画面の例を示す図である。

【図7】DDoS攻撃対策を施さないネットワークを示す図である。

10 【図8】IPヘッダ、TCPヘッダのフォーマットを示す図である。

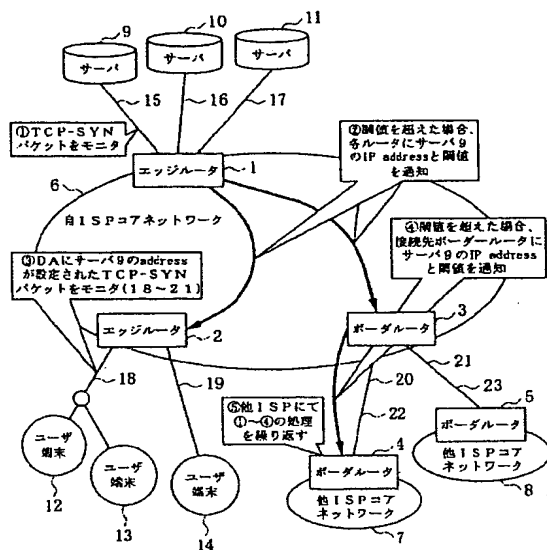
【図9】正常なTCPコネクション処理（3ウェイハンドシェイク処理）のシーケンスチャートである。

【図10】TCP-SYN Floodが行われた場合のシーケンスチャートである。

【符号の説明】

- 1…サーバを収容する自ISPのエッジルータ、
- 2…加入者を収容する自ISPのエッジルータ、
- 3…他ISPと接続するボーダールータ、
- 4～5…他ISPとの接続における他ISP側のボーダールータ、
- 6…自ISPコアネットワーク、7～8…他ISPコアネットワーク、
- 9～11…自ISPにてエッジルータ1に収容されるサーバ、
- 12～14…自ISPにてエッジルータ2に収容されるユーザ端末、
- 15～17…エッジルータ1におけるサーバ9～11側のインターフェース、
- 18～19…エッジルータ2のユーザ端末12～14のインターフェース、
- 20～21…ボーダールータ3の他ISPボーダールータ側インターフェース、
- 22～23…他ISPボーダールータの自ボーダールータ側インターフェース。

【図1】



【図3】

トラフィック閾値設定

起動条件 ☐ 通知要 ☒ 通知不要 51

VIRTUAL ROUTER IDENTITY (記述例: 1, 3, 5-12)

SOURCE ADDRESS ☐ 指定する ☒ 指定しない 52

DESTINATION ADDRESS ☒ 指定する 53 ☐ 指定しない

☐ 直接指定する 54

☐ 通知されたアドレス指定する

PROTOCOL ☒ 指定する TCP 55 ☐ 指定しない

CONTROL FLAGS ☒ 指定する SYN 56 ☐ 指定しない

閾値 ☐ 計算する 計算式 57

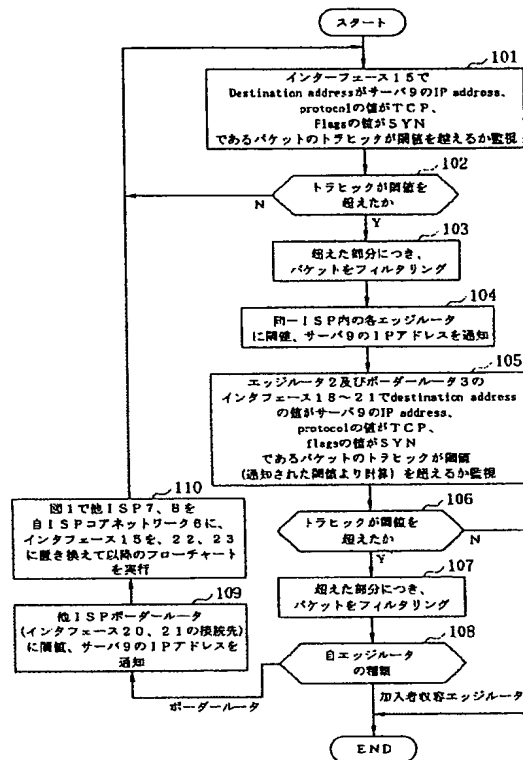
☒ 計算しない 60 Kbps

通知の有無 ☒ 通知する 通知先 IP ADDRESS 58

☐ 通知しない

59 60

【図2】



【図4】

トラフィック閾値設定

起動条件 ☒ 通知要 61 ☐ 通知不要

VIRTUAL ROUTER IDENTITY (記述例: 1, 3, 5-12) 62

SOURCE ADDRESS ☐ 指定する ☒ 指定しない

DESTINATION ADDRESS ☒ 指定する 63 ☐ 指定しない

☐ 直接指定する 64

☐ 通知されたアドレス指定する 65

PROTOCOL ☒ 指定する TCP 66 ☐ 指定しない

CONTROL FLAGS ☒ 指定する SYN 67 ☐ 指定しない

閾値 ☒ 計算する 68 計算式 69

☐ 計算しない Kbps

通知の有無 ☐ 通知する 通知先 IP ADDRESS 70

☒ 通知しない 68

69 70

【図6】

トラヒック閾値設定

81

起動条件 ☒ 通知要 ☐ 通知不要

VIRTUAL ROUTER IDENTITY 22 (記述例: 1, 3, 5-12)

SOURCE ADDRESS ☐ 指定する ☐ 指定しない

DESTINATION ADDRESS ☒ 指定する ~ 83 ☐ 指定しない

☐ 広域指定する

☒ 通知されたアドレス指定する ~ 84

85

PROTOCOL ☒ 指定する TCP ☐ 指定しない

CONTROL FLAGS ☒ 指定する SYN ☐ 指定しない

86

閾値 ☒ 計算する 87 計算式 通知閾値

☐ 計算しない kbps

88

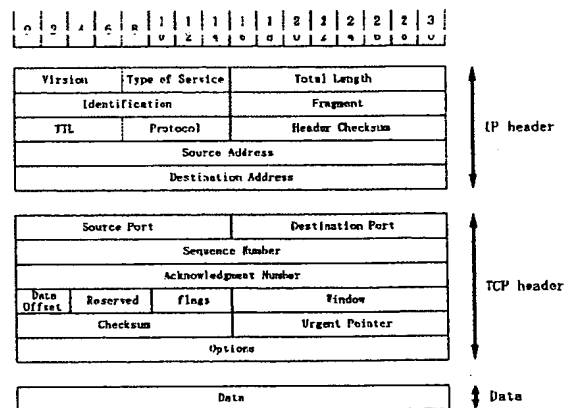
通知の有無 ☒ 通知する 通知先 IP ADDRESS 22.33.44.55
33.44.55.66

☐ 通知しない

89 90

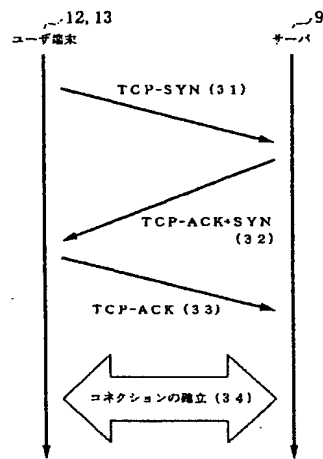
設定 キャンセル

【图8】



※ flagフィールド6bitは、それぞれ、6つの1bitフィールド
URG, ACK, PSH, RST, SYN, FINで構成される。

【図9】



【図10】

